

Security Architecture

5 Background of the Invention

Sub
a1

The present invention relates to the provision of improved security in a device which has services accessible by other devices communicating with the device. It particularly relates to devices which are accessed over a radio interface in accordance with the Bluetooth specification.

Sub
a2

Figure 1 illustrates a network 2 of radio transceiver units, including a master unit 4 and slave units 6, 8 and 10, communicating by transmitting and receiving radio packets. There is only one master in a network. The network operates in a time division duplex fashion. The transceiver units are synchronised to a common time frame determined by the master unit 4. This time frame consists of a series of time slots of equal length. Each radio packet transmitted in the network has its start aligned with the start of a slot and a single packet is transmitted in the network at a time. When the master unit is performing point-to-point communication a transmitted radio packet is addressed to a particular transceiver which replies to the master unit by transmitting a radio packet addressed to the master unit in the next available time slot. When the master unit is performing point to multi-point communication a transmitted radio packet is addressed to all transceiver units. Any time misalignment between the master and a slave is corrected by adjusting the timing of the slave.

Sub
a3

The transceivers transmit and receive, in this example, in a microwave frequency band, illustratively 2.4 GHz. The network reduces interference by changing the frequency at which each radio packet is transmitted. A number

of separate frequency channels are assigned each with a bandwidth of 1MHz, and the frequency may hop at a rate of 1600hops/s. The frequency hopping of the transceivers communicating in or joining the network is synchronised and controlled by the master unit. The sequence of hopping frequencies is unique for the network and is determined by a unique identification of the master unit.

Each transceiver unit has a unique identification, the Unit ID, henceforth referred to as the Bluetooth ID. Each Bluetooth ID (48-bit IEEE address) is unique for each Bluetooth unit. A Bluetooth ID of a unit can be found through an enquiry routine over the RF interface to the unit.

The network is a radio frequency network suitable for transmitting voice information or data information between transceivers. The transmissions made are of low power, for example 0 to 20dBm, and the transceiver units can effectively communicate over the range of a few centimetres to a few tens or hundred of metres.

Referring to Figure 2, a frame 20 is illustrated. This frame 20 is the common time frame used by the network 2 and controlled by the master unit 4. The frame illustratively has slots 22 to 29. The slots designated by even numbers are reserved. Only the master unit can begin transmitting a radio packet aligned with the start of the even numbered slots. The slots designated by odd numbers are reserved. Only radio packets transmitted by a slave, that is radio packets addressed for reception by the master unit can have their start aligned with the start of the odd numbered slots. Each slot is allocated a different one of a sequence of hopping frequencies. It is however, possible for a radio packet to extend over a number of slots and in this case the frequency at which the packet is transmitted remains constant at that allocated to the slot at the start of the packet. A slot has a constant time period and is typically 625 microseconds.

Referring to Figure 3, a typical radio packet 30 is illustrated. The radio packet has a start 32 and contains three distinct portions: a first portion contains an Access Code 34, a second portion contains a Header 36 and a third portion contains a Payload 38. The Payload 38 has a Payload Header 37.

Sub a6

Referring to Figure 4, a schematic illustration of a transceiver unit is shown. Only as many functional blocks and interconnections are shown in this diagram as are necessary to explain in the following how a transceiver unit and the communication network operates. The transceiver unit 40 contains a number of functional elements including: an antenna 46, receiver 50, synchroniser 52, header decoder 54, controller 60, memory 56, packetiser 42, clock 68, frequency hop controller 48 and transmitter 44. Although these elements are shown as separate elements they may in fact be integrated together and may be carried out in software or in hardware.

Sub a7

Data to be transmitted in the payload of a packet by the transceiver unit 40 is supplied as data signal 41 to the packetiser 42. Control information to be transmitted in the payload of a packet is supplied in a payload control signal 87 provided by the controller 60 to the packetiser 42. The packetiser 42 also receives an access code control signal 69 and a header control signal 71 from controller 60 which respectively control the Access Code 34 and the Header 36 attached to the payload to form the packet. The packetiser 42 places the data or control information into a packet 30 which is supplied as signal 43 to the transmitter 44. The transmitter 44 modulates a carrier wave in dependence upon the signal 43 to produce the transmitted signal 45 supplied to the antenna 46 for transmission. The frequency of the carrier wave is controlled to be one of a sequence of hop frequencies by a transmission frequency control signal 47 supplied by the frequency hop controller 48 to the transmitter 44.

009090" E008560

[illegible]

The memory 56 may store applications.

The operation of unit can also be understood from Figure 5 which illustrates a Bluetooth protocol stack 100. The stack 100 includes, in order from the bottom up, the basic layers including RF layer 102, Baseband and Link

Control layer 104, Link Manager Protocol Layer 106 and Logical Link Control and Adaptation Layer (L2CAP)108. The layer L2CAP 108 connects with a number of overlying layers 110 including an Internet layer 112 for providing TCP/IP protocol, a Human Interface Device layer 114 for interfacing with the user interface 130 and a RF Communications layer 116 which emulates serial ports of a PC (com1, com2 com3 etc). Each of the layers 112, 114 and 116 may connect directly with one or more applications/services 118 and are able to multiplex their output so that data is sent to the correct one of several applications/services. The layer L2CAP 108 may also connect directly to an application or service.

In the units currently proposed, the Baseband and Link Control layer 104 enables the physical RF link between units using inquiry and paging to synchronise their clocks and transmission frequencies. The Link Manager Protocol Layer 106, henceforth referred to as the Link Layer 106, is responsible for link set-up between two units including security, control of packet size, connection and power modes. In the proposal the Link Layer 106 responds to the payloads received in Link Management Protocol packets.

L2CAP allows higher level protocols to receive the payloads of received L2CAP data packets. The L2CAP protocol may be coupled to application and higher protocol layers and transfers data between either higher level protocols and services and the lower level Link Layer 106.

The payload header 37 of the payload 38 in packets 30 distinguishes L2CAP packets from Link Management Protocol packets. At present, it is required that the Link Management Protocol packets should be filtered out by the Link Layer 106 and not propagated to higher layers.

005090" E0088560

sub a9 → ~~The Bluetooth technology should provide security measures both at the application layer and the link layer. Currently, in each Bluetooth unit the link layer 106 security measures are standardised. Authentication and encryption routines are implemented in a standard way in each device in the Link Layer 106.~~

sub a10 → ~~Each unit stores one or more secret authentication link keys for use in communication with another unit or units. Typically a unit will permanently store a link key for each of the units it wishes to communicate with. Each link key is associated with the Bluetooth ID of the unit for which it is used to communicate.~~

09588003 060600
The stored secret link key is used in an authentication routine to authenticate the identity of the unit being communicated with. The stored shared secret link key is also used to generate an encryption key. The encryption key is derived from but is different to the authentication link key and a new encryption key is generated each time encryption is used by using a random number generator.

sub a11 → ~~A challenge response scheme is used to authenticate a unit. A valid pair of units share the same secret link key. A first unit produces a random number and challenges a second unit to authenticate itself by supplying the random number to it. The second unit returns the result of a function which takes as its arguments the Bluetooth ID of the second unit, the received random number and the key associated with the first unit but stored in the second unit. The first unit uses the same function to produce a result which if it equals the result received from the second unit authenticates the second device. The function in the first unit takes as its arguments the Bluetooth ID of the second unit which has been previously obtained, the random number and the key associated with the second unit but stored in the first unit.~~

The authentication procedure occurs in the Link Layer of each unit. Once authentication has been successfully completed access to the protocol layer, services and applications in the unit is unrestricted.

5

Each time encryption is required a random number is produced and an encryption key is formed from the random number and the authentication key for the link. The encryption process occurs in the Link Layer 106.

- 10 If the two devices have not previously communicated there will be no shared link key stored in the devices and it is necessary to 'pair' the devices. This may be done by inputting a PIN number into a user interface of the first unit and inputting the same PIN into a user interface of the second unit. The PINs may be used for the calculation of temporary initial authentication link keys
- 15 until the calculation of a permanent shared secret authentication link key for communication between the devices.

- One problem with the presently proposed security system is that it is inflexible. Once the link layer 106 has allowed a device access to the layers
- 20 above it, its access is unrestricted except by specific security features built into the applications themselves. It would be desirable to provide an improved, more flexible, security system.

Summary of the Invention

25

- According to one aspect of the present invention there is provide a device for communicating with other devices to allow them to access applications, comprising: at least a first application; authentication means for authenticating a communicating device; access control means accessible by a
- 30 communicating device requesting access to the first application without the

communicating device having been authenticated by the authentication means, and arranged to arbitrate whether access of the communicating device to the first application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the access control
5 means instructs the authentication means to authenticate the communicating device.

According to another aspect of the present invention there is provided a device for communicating with other devices to allow them to access
10 applications, comprising: at least first and second applications; authentication means for authenticating a communicating device; first access control means accessible by a communicating device requesting access to the first application without the communicating device having been authenticated by the authentication means, and arranged to arbitrate whether access of the
15 communicating device to the first application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the access control means instructs the authentication means to authenticate the communicating device. second access control means accessible by a communicating device requesting access to the second application without
20 the communicating device having been authenticated by the authentication means, and arranged to arbitrate whether access of the communicating device to the second application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the access control means instructs the authentication means to authenticate the
25 communicating device, wherein the first access control means is accessible by a communicating device requesting access to the second application without the communicating device having been authenticated by the authentication means, and is arranged to provide the access of the communicating device to the second access means.

According to another aspect of the present invention there is provided a method of arbitrating the access of a requesting device to a service provided by a providing device comprising: sending a request to access the service
5 from the requesting device to the providing device; receiving the request at the providing device and passing it, without authenticating the requesting device, to an arbitration means interfacing the service; determining, in the arbitration means, whether to grant or refuse access to the first application by the requesting device, wherein if the determination requires an authentication
10 of the requesting device, the authentication is performed during that determination and not previously.

Embodiments of the invention provide a flexible security architecture that performs access checks when connection to a service is requested including,
15 if necessary, authentication and encryption at the time of requesting access to application. The access control means may be a multiplexing protocol layer and the authentication means may be the link layer.

It is preferable that a device requesting access to a service is authenticated
20 once and not many times. This may be achieved by having the request for access to a service arbitrated once-only, preferably in response to a query from the highest possible multiplexing layer (the one that directly interfaces the service).

25 Access to a service may be arbitrated in dependence on the security requirements of the requested service and/or the trust level of the device requesting access. The security architecture is implemented without changing the basic functions (pairing, authentication, encryption) which remain in the authentication means (link level).

Sub
a12

According to a further aspect of the present invention there is provided a device for providing services and allowing access by other devices to the provided services, comprising: an interface for communicating with the other devices and receiving requests to access a service therefrom; arbitration means, for determining whether a requesting device communicating through the interface can access a service it has requested access to, arranged to store trust indications in association with requesting devices and arranged to receive from the interface an indication, originating from the other device, identifying the other device, wherein, if the requesting device has a stored trust indication associated therewith no user authorisation is required and if the requesting device has no stored trust indication associated therewith user authorisation is requirable; and a user interface for providing user authorisation.

Sub
a13

According to a further aspect of the present invention there is provided a device for providing services and allowing access by other devices to the provided services, comprising: an interface for communicating with the other devices and receiving requests to access a service therefrom; arbitration means, for determining whether a requesting device communicating through the interface can access a service it has requested access to, arranged to store trust indications in association with requesting devices and store security indications in association with provided services and arranged to receive from the interface indications, originating from the other device, identifying the other device and the service requested, wherein, if the requesting device has a stored trust indication associated therewith no user authorisation is required and if the requesting device has no stored trust indication associated therewith user authorisation is required in dependence upon the stored security indication associated with the requested service; and a user interface for providing user authorisation.

009090" 00088560

Sub
a 14

11

~~According to embodiments of the invention, access to services depends upon~~
the trust level of the device which is trying to access the service. A trusted
device, once its identity has been verified has access to all the
services/applications. A not-trusted device may require user authorisation
5 each time it attempts to access a service. Therefore the grant of access of a
not-trusted device to one service does not open up the other services to
access. Separate user authorisation is required to access each of the other
~~services.~~

10 Brief Description of the Drawings

For a better understanding of the present invention and to understand how
the same may be brought into effect reference will now be made by way of
example only to accompanying drawings in which:

15

Figure 1 illustrates a communications network including a master and slave
units;

Figure 2 illustrates the time frame of the communications network;

Figure 3 illustrates a radio packet

20 Figure 4 illustrates a transceiver unit suitable for use as a master or slave;

Figure 5 illustrates a protocol stack used by a transceiver unit;

Figure 6 illustrates a security architecture;

Figures 7a and 7b illustrate, respectively, a service database and a device
database;

25 Figures 8a and 8b illustrate information flow in the security architecture when
access for a not-open service is requested by a trusted and untrusted device
respectively

Figures 9 to 11 are flow diagrams illustrating the arbitration process
performed by the controller to determine if a device should access a service.

30

Detailed Description

- 5 Figure 6 illustrates a security architecture in accordance with one embodiment of the invention. The Bluetooth protocol stack 100 is illustrated. It includes lower layers including the link layer 106, a lowest multiplexing protocol layer 108 such as the L2CAP layer, a higher multiplexing protocol layer 110 such as the RFCOMM layer 116 and an application layer 118. Also illustrated are
10 the User Interface 130, a security manager 120, a service database 122 and a device database 124.

- The link layer 106 is directly connected to the lowest multiplexing protocol 108. Access to the higher multiplexing protocol 110 and the
15 applications/services 118 from the link layer can only be achieved via the lowest multiplexing protocol layer 108.

- The lowest multiplexing protocol layer 108 is directly connected to the higher multiplexing protocol 110 and also directly connected to application 118₃.
20 Access to the application 118₃ can be made directly by the lowest multiplexing protocol, whereas access to applications 118₁ and 118₂ can only be made via the higher multiplexing protocol 110 which is directly connected to applications 118₁ and 118₂.

- 25 When a packet is received by a unit, the payload of the packet is passed to the lowest multiplexing protocol layer 108. The payload is not filtered by the link layer 106. If the received packet is a request to access a service/application, access to that service application is arbitrated.

sub
a's

Sub
a₁₄

application. If access is denied, the Security Manager 120 sends a refusal signal to the querying protocol layer 110 preventing access of the requesting unit to the desired service.

- 5 The lowest multiplexing protocol 108 makes an enquiry to the Security Manager for every received request for access to a service. The request is allowed to progress to a higher layer or service only if access is granted by the Security Manager. Each of the multiplexing protocol layers through which a request to access a service is routed, makes an enquiry to the Security
- 10 Manager each time a request is received. The request is allowed to progress to a higher layer or service only if access is granted by the Security Manager. No application/service can therefore be accessed by a unit without at least one arbitration by the Security Manager.
- 15 The Security manger 120 is a software module with interfaces to protocols 108 and 110, services/applications 118, the UI 130, the databases 122 and 124 and the link layer 106. The security manager controls the link layer and the performance of its standard functions such as authentication, encryption and pairing. The Security Manager knows the identity of the services each of
- 20 the protocol layers has direct access to.

- Sub
A17
- 25 The Security Manager may use its interfaces to the service database 122, the device database, the link manager and the UI 130 to perform an above-mentioned arbitration. An exemplary service database is illustrated in Figure 7a and an exemplary device database is illustrated in Figure 7b. When the Security Manager receives a query from the protocol layers or applications it queries the databases 122 and 124. It accesses the fields associated with the requested application/service from the service database and accesses the fields associated with the Bluetooth ID of the requesting unit from the device
 - 30 database 124.

009090" 0008560

Sub
Q18

~~The databases are used to define different security levels for devices and services. Each unit has a device database which stores information about other devices it has previously communicated with. The device database has~~

5 an entry for each Bluetooth ID of the other devices. Each entry has associated fields including a first field to indicate whether that device is trusted or not trusted, a second field for storing the current link key for communication with that devices and a third field to indicate whether there

~~has been a successful authentication with that device in the current session.~~

10

The trusted field is binary and there are therefore two security levels for devices- trusted and not-trusted. If a first unit records a second unit as trusted in its device database, then that second unit can access all the services of the first unit after authentication. If the first unit records the second unit as not-

15 trusted (untrusted), the second unit may have its access to the services of the first unit restricted in dependence upon the service database in the first unit.

Each unit has a service database (Figure 7a) which stores information about the applications and services in that unit available for access by another unit.

20 The service database has an entry for each available application or service. Each entry has associated fields including a first field to indicate whether that service is open or not open and a second field to indicate whether encryption is required. This security information can be provided by the services/applications to the security manager during a registration procedure.

25

The Security Manager defines three levels of security in relation to a service. What the level is depends upon the security rating of the service (open/ not-open) and the security rating of the requesting device (trusted/untrusted). When the security rating of the service is open there is no dependence upon

0058003 060500
009090" E0088560

whether the requesting device is trusted or untrusted and the open services are open to all devices.

sub
Q19
5 ~~When the security rating of the service is not open then there is a~~
dependence upon the trust level of the device requesting access. If the
requesting device is trusted, then the device requesting access to the service
must be authenticated before access to the service is granted. If the
requesting device is untrusted, then the device requesting services must be
authenticated and then explicit user authorisation must be given before
10 ~~access to the service is granted.~~

Referring to the flow diagrams in Figures 9 to 11, after the Security Manager
receives an query (200) from the multiplexing protocol layers 108 or 110, it
determines whether the querying multiplexing layer is directly connected to
15 (interfaces with) the requested service (201). If the query from the protocol
layer concerns a service to which the protocol layer is not directly connected,
but is indirectly connected through higher multiplexing protocol layers, the
Security Manager allows the passage of the request to the higher multiplexing
protocol layer by sending a grant signal to the querying protocol layer. If the
20 query from the querying protocol layer concerns a service to which the
querying protocol layer is directly connected, the Security Manager performs
an arbitration to determine if access to the service should be allowed or
denied.

25 The arbitration is initiated by the Security Manager accessing (202) the
databases 122 and 124, identifying whether the requesting device is trusted
and identifying whether the requested service is open (204).

If the requested service is an open service, the Security Manager grants
30 access (216) by sending a grant signal to the querying protocol layer which

009090" 000000

then accesses the requested application. If the requested service is not an open service the arbitration continues.

If the requesting device is trusted, authentication only is required. If authentication of the requesting device has not occurred in this session (206) (determined from the 3rd field of the entry for the requesting device in the device database), then the security manager instructs the link layer 106 to perform an authentication (208). Referring to Figure 10, the security manager provides the link layer with the current key (if any) stored in the 2nd field of the database entry. The link layer performs the authentication (with pairing if necessary) and informs the security manager if the authentication has been successful. The processes of pairing (222), checking the link key is current (224) and creating a link key are implementation dependent and are not described further. If the authentication is unsuccessful the Security Manager sends (218) a refusal signal to the querying protocol thereby preventing access to the requested service. If the authentication is successful, link layer also returns the current link key for the requesting device. The Security Manager then updates (210) the device database, placing the current link key in the second field of the database entry and indicating that successful authentication has occurred in this session in the third field of the entry. The Security Manager then determines (212) whether the requesting device is a trusted device. As the device is trusted the Security Manager sends (216) a grant signal to the querying protocol thereby allowing access to the service.

Sub Q20

~~25 If the requesting device is not trusted, authentication and user authorisation is required. If authentication of the requesting device has not occurred in this session (206) (determined from the 3rd field of the entry for the requesting device in the device database), then the security manager instructs (208) the link layer 106 to perform an authentication. The security manager provides the~~

30 link layer with the current key (if any) stored in the 2nd field of the database

005000 000000

entry. The link layer performs the authentication (with pairing if necessary) as previously described in relation to Figure 10, and informs the security manager if the authentication has been successful. If the authentication is unsuccessful the Security Manager sends (218) a refusal signal to the querying protocol thereby preventing access to the service. If the authentication is successful the link layer also returns the current link key for the requesting device and the Security Manager updates the device database (210), placing the current link key in the second field of the database entry and indicating that successful authentication has occurred in this session in the third field of the entry. The security manager checks (212) the trusted status of the requesting device. As the device is not-trusted, the security manager then attempts to obtain user authorisation (214) as illustrated in Figure 11. The security manager controls (230) the UI 130 to indicate to the user that some positive act is required to allow a requesting device access to a service. The service and/or the requesting device may be identified on a screen. The user can agree or disagree to the access. Agreement causes the Security Manager to give (216) a grant signal to the querying protocol layer thereby allowing access to the requested service. Disagreement causes the Security Manager to give (218) a rejection signal to the enquiring protocol thereby preventing access to the requested service. The fact that user authorisation has been given is not recorded and access is therefore one time only. The Security Manager, may then as an option, offer (232) the user the opportunity to change the trust status of the requesting device from untrusted to trusted with subsequent updating (234) of the device database.

25

If encryption is required in addition to authentication, the Security Manager controls the link layer 106 to perform it, before allowing connection to the application/service requested.

The applications/services 118 and the higher multiplexing protocol 110 must register their multiplexing policies with the Security Manager so that it can determine which application/service is directly connected to each protocol layer.

5

The process of accessing a service using a trusted device is further illustrated in Figure 8a. The protocol layer is directly connected to a service.

1. Connect request to protocol layer
2. If access control occurs at this protocol layer, then send enquiry to Security Manager
3. Security manager looks up service database
4. Security manager looks up device database
5. Security Manager enforces standard authentication (and possibly encryption) in the link layer
6. Security Manager grants access or link terminated
7. Protocol layer continues to set up the connection by contacting higher protocol layers/ services

The process of accessing a service using an untrusted devices is further illustrated in Figure 8b. The protocol layer is directly connected to a service.

1. Connect request to protocol layer
2. If access control occurs at this protocol layer, then send enquiry to Security Manager
3. Security manager looks up service database
4. Security manager looks up device database
5. Security Manager enforces standard authentication (and possibly encryption) in the link layer
6. ~~Security Manager asks for manual user authorisation~~
7. Security manager may update device database (trusted?)
8. Security Manager grants access or link terminated

sub
a21

In this embodiment authentication (5) is performed before authorisation (6). It would of course be possible to perform authorisation (6) before authentication

$$\text{Sub } a_{22}$$

10

Sub
a23

15

20

25

Sub
A24

sub
a25

5

15

THE UNIVERSITY OF CHICAGO